CONTENTS

WTO Commentary

WTO COMMENTARY

Coherent International Trade Policies Hasten, Not Retard, Cloud Computing

Lawrence A. Kogan*

Amid the apparent global economic slowdown affecting multiple goods and services sectors, including those comprising the broad rubric of ICTs, the availability of ubiquitous multiple broadband and Internet-based cloud offerings continue to present national and regional governments with a significant potential source of current and future local economic growth and job creation possibilities. While governments cognizant of this opportunity have endeavoured to exploit it, they have, however, largely remained cautious in addressing emerging public policy concerns surrounding third country digital transfers of individual and business data to the cloud. A number of governments have embraced different and often inconsistent regulatory and voluntary approaches in answer to these data/informational privacy and data security concerns. These responses have imposed significant direct and indirect restrictions on trans-border data flows that have had the undesirable effect of retarding the adoption of cloud computing service platforms in various markets. More established globally-focused cloud service providers have been most adversely impacted by these new measures, even after having previously reformed their IP-based business models to satisfy foreign governments' expressed preference for less expensive royalty-free ICT interoperability frameworks. Consequently, these and other companies, increasingly suspicious of disguised protectionism at play, have called upon governments to quickly reach consensus in one or more multilateral, regional and/or bilateral forums on an open, transparent and non-trade-restrictive framework capable of providing a positive enabling environment that facilitates the eventual expansion of international cloud computing.

I A GATHERING STORM

Media reporting increasingly assessing the key pillars of the global economy – (Asia (China[1]), the European Union (EU)[2] and the United States (US[3])) – to be slowing[4] and possibly already in or heading toward recession are compelling.[5] Surprisingly, even the rapidly converging telecommunications and IT sectors which have been 'widely seen as an engine for development and an indispensable tool for economic growth',[6] appear to have been adversely impacted by this downturn, with the traditional computer, related hardware, and mobile phone

Notes

* Lawrence A. Kogan is a Managing Attorney of The Kogan Law Group, P.C., a New York City-based multidisciplinary professional services firm, and the President/CEO of the Institute for Trade, Standards and Sustainable Development (ITSSD), a Princeton, NJ-based nonprofit legal research, analytics and educational organization.

1 *See China's Manufacturing Growth Weakens As New Orders Drop*, Bloomberg News , http://www.bloomberg.com/news/2012-07-01/china-june-manufacturing-pmi-50-2-vs-economists-est-49-9.html(July 1, 2012); Markit, *HSBC PMI Paints Worrying Growth Picture*, Markit China Economic Research, http://www.markit.com/assets/en/docs/commentary/markit-economics/2012/jun/CN_NOTE_21_06_12.pdf (June 21, 2012).

2 *See* Markit, *Steepest Drop in German Private Sector Output for Three Years; Euro Crisis Leads to Survey-Record Monthly Fall in Service Providers' Business Outlook*, Markit Flash Germany PMI Press Release, http://www.markit.com/assets/en/docs/commentary/markit-economics/2012/jun/DE_Composite_ENG_1207_FLASH.pdf (June 21, 2012).

3 *See* Kathleen Madigan, *U.S. Manufacturing Activity Plunges*, Wall Street J.,http://online.wsj.com/article/SB10001424052702304211804577502543898983040.html (July 2, 2012); Himanshu Singh, *Overnight Markets: US Stocks Tumble Amid Global Manufacturing Slowdown*, Citywire.com , http://citywire.co.uk/money/overnight-markets-us-stocks-tumble-amid-global-manufacturing-slowdown/a598349?ref=citywire-money-latest-news-list (June 22, 2012); Markit, *PMI Signals Weakest Manufacturing Expansion in 11 Months*, Markit Flash U.S. Manufacturing PMI News Release, http://www.markit.com/assets/en/docs/commentary/markit-economics/2012/jun/US_Manufacturing_ENG_1207_FLASH.pdf (June 21, 2012).

4 *See* Markit, *Flash Manufacturing PMI Surveys-Manufacturing Surveys Turn Down in the US*, Eurozone and China, Markit Economic Research, http://www.markit.com/assets/en/docs/commentary/markit-economics/2012/jun/NOTE.pdf (June 21, 2012).

5 *See* Rex Nutting, *Despite Slowdown, Recession Not Inevitable*, MarketWatch, http://articles.marketwatch.com/2012-06-21/commentary/32344273_1_manufacturing-index-outright-contraction-global-economy (June 21, 2012); Mike Shedlock, *12 Reasons Why The US Recession Has Already Arrived*, BusinessInsider, http://www.businessinsider.com/12-reasons-us-recession-has-arrived-2012-6 (June 21, 2012).

6 *See* World Trade Organization Council for Trade in Services, *Telecommunication Services – Background Note by Secretariat*, (S/C/W/299) at par. 5, *citing* Gareth Locksley, *The Media and Development - What's the Story?*, World Bank Working Paper No. 158 (2009), http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/The_Media_and_Development.pdf (June 10, 2009).

products segments suffering from a sizeable decline in new orders.[7]

2 Cloud computing's economic silver lining

If there is a silver lining in all of this, it involves broadband-based cloud computing *services*. Cloud computing is currently considered one of the few remaining bright spots in the IT services sector[8] that has proven resilient and capable of 'generating strong job demand',[9] improved business productivity and cost savings[10] for all companies, including small and medium sized enterprise (SME) users in recession-plagued Europe.[11] During 2010 for example, the global market for public cloud computing was estimated at between USD 14 billion–USD 15 billion, with projections for 2015 ranging from USD 43.3 billion to USD 94.1 billion.[12] In addition, cloud-based advertising service revenues which subsidize 'many cloud-based applications that consumers use for free', were estimated at USD 36.5 billion in 2010, and are projected to be USD 77.1 billion in 2015.[13]

3 Cloud computing conceptualized

The U.S. National Institute of Science and Technology (NIST) defines cloud computing as 'a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'.[14] NIST has described cloud computing as including the following five characteristics: (i) on-demand self-service; (ii) broad network access; (iii) resource pooling; (iv) rapid elasticity or expansion; and (v) measured service.[15] It has also found that cloud computing entails the following three types of services, which may or may not be fee-based: (i) software-as-a-service (SaaS) which is 'comprised of any software application accessed through the cloud'; (ii) platform-as-a-service (PaaS) which is 'a cloud-based service for programmers to create or customize software applications'; and (iii) infrastructure-as-a-service (IaaS) which 'provides basic computing functions such as data storage and processing via the cloud'.[16] Cloud services can also be provided in a more private setting to one or more users consistent with user privacy and security requirements, or hosted in-house within a single user.[17] Given the ubiquity of digital data transfers over the Internet and the Internet's evolved architecture, digital data can be easily (intentionally or unintentionally) transferred across national borders.[18]

4 Governments recognize economic potential of cloud computing

Economists have estimated that 'SaaS will account for 6.1 percent of global software sales [USD $21.3B/$347B

Notes

7 *See Tech Sell Off Might Be Near*, TechTerse, http://www.techterse.com/2012/02/tech-sell-off-might-be-near.html (Feb. 28, 2012). *See also*, Tim Weber, *Why Smartphones Are Not Suffering In The Recession*, BBC News, http://news.bbc.co.uk/2/hi/8292101.stm (Oct. 6, 2009).

8 *See Tech Sell Off Might Be Near*, *supra* n. 7. *See also* World Trade Organization Council for Trade in Services, *Telecommunication Services – Background Note by Secretariat* (S/C/W/299), *supra* n. 6 at para. 6.

9 *See Yoh Index Finds Bright Spots and Anomalies in Labor Market, Even in Face of Disappointing BLS Jobs Report*, BusinessWire, http://www.businesswire.com/news/home/20120612005397/en/Yoh-Index-Finds-Bright-Spots-Anomalies-Labor (June 12, 2012).

10 *See* Humayun Shahid, *The Cloud Effect: A Dent In Traditional Software Pricing*, CloudTweaks.com, http://www.cloudtweaks.com/2012/06/the-cloud-effect-a-dent-in-traditional-software-pricing/ (June 22, 2012); Mitchell Osak, *Cloud Computing Disrupts Software Pricing*, Financial Post, http://business.financialpost.com/2012/06/20/cloud-computing-disrupts-software-pricing/(June 20, 2012).

11 *See* Daniel Saks, *How Cloud Computing is Driving Success for Europe's Small Businesses*, The Guardian, http://www.guardian.co.uk/media-network/media-network-blog/2012/jun/21/cloud-computing-small-businesses-europe (June 21, 2012). *See also* Centre for Economics and Business Research, *The Cloud Dividend: Part One - The Economic Benefits of Cloud Computing to Business and the Wider EMEA Economy*, Executive Summary at p.7, http://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf (December 2010).

12 *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, J. Intl. Com. Econ., 21(May 2012), http://www.usitc.gov/journals/policy_challenges_of_cross-border_cloud_computing.pdf. *See also* Bloomberg News, *Amazon Rival Rackspace Evokes Dot-Com Era Deal: Real M&A*, http://www.bloomberg.com/news/2012-06-20/amazon-rival-rackspace-evokes-dot-com-era-deal-real-m-a.html(June 20, 2012).

13 *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n. 12 at p. 7.

14 *See* Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology Special Publication 800-145 (Sept. 2011), at p. 2, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. *Cf.* European Commission Expert Group Report, *The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010*, Public version 1.0 at p. 8, http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf (Jan. 26, 2010).

15 *See* National Institute of Science and Technology Information Technology Laboratory, *Final Version of NIST Cloud Computing Definition Published*, NIST Tech Beat, http://www.nist.gov/itl/csd/cloud-102511.cfm (Oct. 25, 2011).

16 *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n. 12 at p. 4.

17 *Id.*

18 *See* Christopher Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, OECD Digital Economy Papers, No. 187 (2011) at pp. 10–11, http://dx.doi.org/10.1787/5kg0s2fk315f-en.

billion} while IaaS and PaaS will account for 2.2 percent of global IT services sales {USD$22B/$983B} in 2015.'[19] A number of national and regional governments within the EU have increasingly recognized the promise of cloud computing and its contribution to the growth in worldwide internet and smart phone use, and have endeavoured through development of law and policy frameworks to harness the potential it offers for further market and overall regional economic growth.[20] EU Digital Agenda Commissioner Neelie Kros recently noted that 'the Cloud means a big boost to our economy. In a country like Germany, some estimate that over five years, Cloud computing could generate over €200 billion in economic benefits, and 800,000 jobs'.[21] In addition, a recently released European 'cloud readiness report' revealed that there is a growing acceptance and usage of private cloud services among businesses, especially those operating in the telecom and media sectors.[22] Some Asian governments, as well, have sought to promote growth in cloud computing at both the regulatory and infrastructure levels. For example, a recent assessment of 'cloud readiness'[23] within Asia found that Asian markets 'known for their aggressive economic and technological development' were the most prepared and able to exploit cloud computing (i.e., Japan, followed by Hong Kong, South Korea and Singapore),[24] and that among the ten attributes comprising such readiness index '[g]overnment influence…represent[ed] 60% of the overall ranking'.[25] Moreover, a recently released London School of Economics (LSE) study[26] reaffirms how infrastructure (e.g., energy) costs, as indirectly indicative of government policy choices,[27] can be a key determinant of where cloud computing companies decide to establish data centre facilities and cloud-related jobs are ultimately created. The LSE study, which assessed the overall economic impact of cloud computing in the aerospace and smart phone services sectors within the United States, the United Kingdom, Germany and Italy, found that, 'as a result of distinctly favorable cost structures and labor productivity in North America, especially as regards energy prices . . . 50% of public cloud jobs and 10% of private cloud jobs in the EU {in these sectors} will be generated abroad (mainly in the US)'.[28] According to the study, this translates into 'US cloud-related smartphone services jobs…grow{ing} from 19,500 in 2010 to 54,500 in 2014.'[29]

5 Governments 'seed' cloud computing differently

While governments have become increasingly eager to exploit the potential economic benefits of cloud computing, they have largely remained cautious in addressing public policy concerns surrounding cross-border digital transfers of individual and business data to the cloud. For example, data/informational privacy issues have arisen over how to maintain control over the collection, processing, and dissemination of individuals' personal data by cloud providers and other businesses intent upon using that data commercially (i.e., for purposes of personalizing goods and services, data-mining, etc.) in exchange for low or no-cost cloud service offerings.[30] In addition, data security issues have arisen over how to 'ensur[e] that unauthorized third parties do not obtain access to sensitive {and confidential} data'[31] transferred to the cloud by individuals (e.g., health and financial records, emails, etc.) and businesses (e.g., financial, intellectual property, transactional records, emails, etc.), especially, foreign governments intent upon

Notes

[19] *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n.12 at p. 10, fn20.

[20] *See, e.g.*, Viviane Reding, *Outdoing Huxley: Forging a High Level of Data Protection*, SPEECH/12/464 (6/18/12), Europa Press Release, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/464&format=HTML&aged=0&language=EN&guiLanguage=en. *See also* Matthew Goodrick, *GSA Presentation on Federal Cloud Computing Initiative*, Software & Information Association Conference, http://www.siia.net/cloudgov/ (June 17, 2010); Lutz Schubert, Keith Jeffery & Burkhard Neidecker-Lutz, *The Future of Cloud Computing Opportunities for European Cloud Competing Beyond 2010*, Expert Group Report, Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit (2010), at Executive Summary, pp. 3–4, p. 6, http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf.

[21] *See Neelie Kroes: A European Cloud Strategy*, REDAZIONE MEDIALAWS, http://www.medialaws.eu/neelie-kroes-a-european-cloud-strategy/ (June 25, 2012).

[22] *See* Oracle, *European Cloud Readiness Report: Business Cutting Through the Hype to Find a Strategy that Works for Them*, https://emeapressoffice.oracle.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=2006 (March 2012).

[23] *See* Asia Cloud Computing Association, *Cloud Readiness Index*, http://www.asiacloud.org/docs/CloudReadiness_WhitePaper_Dec11.pdf (Sept. 2011).

[24] *See* Roger Strukhoff, *Asia Cloud Report Offers Benchmarks, No Surprises*, Cloud Computing J., http://cloudcomputing.sys-con.com/node/1975662 (Sept. 10, 2011).

[25] *See* Roger Strukhoff, *Governments Foster Cloud Development in Asia*, Cloud Computing J., http://cloudcomputing.sys-con.com/node/1975873 (Sept. 11, 2011).

[26] *See* Jonathan Liebenau et al., *Modelling the Cloud: Employment Effects in Two Exemplary Sectors in the United States, the United Kingdom, Germany and Italy*, LSE-Enterprise, http://www2.lse.ac.uk/management/documents/LSE-Cloud-report.pdf (January 2012).

[27] *Id*., at Executive Summary, at p. 3, p. 61.

[28] *Id*., at p.15 fn 8, pp. 32, 35-36.

[29] *Id*., at Executive Summary, p. 3, p. 37.

[30] *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n. 12 at p. 7.

[31] *Id.,* at p. 16.

collecting data for statistical, law enforcement and/or national security purposes[32] (e.g., the United States Patriot Act).[33]

Governments have adopted different approaches to address these data/informational privacy and data security concerns. For example, the US Government, which has appeared more focused on promoting economic efficiency, has continued to embrace a non-binding self-regulatory approach '(with sector-specific regulations for certain sensitive types of data)'[34] that aims to[35] and has actually facilitated rapid growth in low- or no-cost cloud service offerings, as well as new jobs.[36] The US approach arguably adopts a 'default position' that presumes that data flows should generally be allowed unless regulators have reason to block or limit them.[37] Other governments, such as the EU's regional institutions and Member State national governments, have taken a more interventionist approach (marked by a greater public sector role[38]) that appears more focused on protecting a defined 'fundamental right'[39] of consumer privacy[40] through adoption of strict binding legislation/regulations.[41] The EU approach aims to facilitate growth in cloud computing services by fostering greater individual and business consumer 'trust' in cloud computing via more stringent governmental oversight of cloud service providers.[42] It arguably adopts a 'default position' that presumes 'that personal data may not flow outside the jurisdiction unless a particular legal basis is present',[43] which commentators have characterized as 'extraterritorial' in design and effect.[44]

The US approach to data protection has arguably remained consistent with the earliest international and regionally-based voluntary (non-binding) self-regulation regime – the Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines),[45] which reflects a similar default position.[46] The US

Notes

[32] *See* Stephen J. Kobrin, *The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance*, The Wharton School, University of Pennsylvania at p. 6, http://knowledge.wharton.upenn.edu/papers/1080.pdf.

[33] *See* Florence de Borja, *Why Is Europe Not Storming The Cloud?*, CloudTweaks.com, http://www.cloudtweaks.com/2012/06/why-is-europe-not-storming-the-cloud/ (June 20, 2012). *See also* Melissa Branzburg, *The Numbers Have It, the U.S. Will Benefit From Cloud Computing*, Mass High Tech, http://www.masshightech.com/stories/2012/03/12/daily18-The-numbers-have-it-the-US-will-benefit-from-cloud-computing.html (Mar. 13, 2012); Noah Gamer, *EU Proposes Data Protection Overhaul; Criticism Ensues*, SimplySecurity.com, http://www.simplysecurity.com/2012/02/03/eu-proposes-data-protection-overhaul-criticism-ensues/ (Feb. 3, 2012); *EU-US Data Privacy Storm Blows Cloud Off Course*, EuraAtiv.com, http://www.euractiv.com/specialreport-cloud-computing/eu-us-data-privacy-storm-blows-c-news-509134 (Nov. 30, 2011).

[34] *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n. 12 at pp. 10–11. *See also* Stephen J. Kobrin, *The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance*, *supra* n. 32 at p. 8.

[35] *See* Stephen J. Kobrin, *The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance*, *supra* n. 32 at pp. 6–7.

[36] *See* Jonathan Liebenau et al., *Modelling the Cloud: Employment Effects in Two Exemplary Sectors in the United States, the United Kingdom, Germany and Italy*, *supra* n. 26 at p. 37; Joe McKendrick, Cloud Computing Fueling Global Economic Growth: London School of Economics Study, Forbes.com, http://www.forbes.com/sites/joemckendrick/2012/01/27/cloud-computing-fueling-global-economic-growth-london-school-of-economics-study/ (Jan. 27, 2012).

[37] *See* C. Kuner, (2011), *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, *supra* n. 18 at p. 8.

[38] *See* Horace E. Anderson, *The Privacy Gambit: Toward a Game Theoretic Approach to International Data Protection*, 9 Vand. J. Ent. & Tech. L. 1, 16 (2006), http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1395&context=lawfaculty.

[39] *See* European Commission, *A Comprehensive Approach On Personal Data Protection in the European Union*, Communication From the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final (Nov. 4, 2010) at Sec. 1, p. 2; Sec. 2.1.1, p. 5; Sections 3, 18, accessible at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

[40] *Id.,* at Sec. 1, p.2, *citing* The European Commission DG Justice, Freedom and Security, *Study On the Economic Benefits of Privacy-Enhancing Technologies (PETs)*, Final Report (July 2010) at Executive Summary at p. xiv, accessible at: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf.

[41] *See* Carl Felsenfeld, *Unnecessary Privacy*, 25 Suffolk Transnatl. L. Rev. 365, 370 (2002); Michael L. Rustad & Thomas H. Koenig, *Harmonizing Cybertort Law For Europe and America*, 5 J. High Tech. L.13, 60 (2005), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=935092&download=yes.

[42] *See* Edelman, *Privacy and Security: The New Drivers of Brand, Reputation and Action Global Insights 2012* (March 2012), Executive Summary at p. 4, http://datasecurity.edelman.com/wp-content/uploads/2012/03/Data-Security-Privacy-Executive-Summary.pdf. *See also* Neelie Kros, *The Clear Role of Public Authorities in Cloud Computing*, Digital Agenda Blog, http://blogs.ec.europa.eu/neelie-kroes/public-authorities-and-cloud/ (Mar. 25, 2011).

[43] *See* C. Kuner, (2011), *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, *supra* n. 18 at pp. 9, 22.

[44] *See* Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 Fordham Intl. L.J. 2024 (1998), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1641&context=ilj.

[45] *See* Organization for Economic Cooperation and Development, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 23, 1980), OECD website at: http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html (accessed Aug. 23, 2012) Paragraph 6 of the OECD Privacy Guidelines clearly reflects that the guidelines are intended to serve only as "minimum standards" for privacy protection that can be "supplemented by additional measures for the protection of privacy and individual liberties" at the national or regional levels. Id. at par. 6. *See also* C. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, OECD Digital Economy Papers, No. 187, (OECD Publishing 2011), http://dx.doi.org/10.1787/5kg0s2fk315f-en. See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, supra n. 18 at paras. 17–18.

[46] While the OECD Privacy Guidelines contain eight privacy principles for national implementation (paras. 7-14), they also contain four principles for international implementation (paras. 15-18) which presume (reflect a 'default position') that trans-border flows of personal data are generally to be permitted except in certain prescribed instances where regulators may block or limit them. *See Annex to the Recommendation of the Council of 23 September 1980: Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data*, Parts Two and Three, OECD website at: http://www.oecd.org/redirect/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (accessed Aug. 26, 2012). *See also* Christoper Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, OECD Digital Economy Papers, No. 187, (OECD Publishing 2011) at p. 22, http://dx.doi.org/10.1787/5kg0s2fk315f-en (accessed Aug. 23, 2012). *See also* Organization for Economic Cooperation and Development, *OECD RECOMMENDATION OF THE COUNCIL ON PRINCIPLES FOR INTERNET POLICY MAKING* (Dec. 2011), http://www.oecd.org/redirect/dataoecd/11/58/49258588.pdf ; http://usoecd.usmission.gov/june2011_internet2.html (accessed Aug. 26, 2012) ("The Council…[r]ecommends that, in developing or revising their policies for the Internet Economy, Members, in co-operation with all stakeholders, take account of the following high level principles…: *1. Promote and protect the global free flow of information; 2. Promote the open, distributed and interconnected nature of the Internet; 3. Promote investment and competition in high speed networks and services;*

approach also dovetails with the more modern Asia Pacific Economic Cooperation (APEC) Privacy Framework,[47] which aims to encourage the development of appropriate information privacy protections while ensuring the free flow of information in the Asia Pacific region.[48] The variability inherent in the APEC Framework, however, has resulted in international legal uncertainty. Since it is recognized as offering less than a uniform approach, it is 'unclear how many members will implement it; in fact, at present APEC members have their own [varied] approaches to privacy protection'.[49] The EU Data Protection Directive's mandatory/regulatory approach has also been similarly non-uniform in application given the discretion its accords EU Member States to render 'adequacy' determinations. This feature, along with the Directive's additional compulsory imposition upon cloud service providers of quite stringent and burdensome compliance obligations, have arguably served to dampen the cloud computing industry and related job growth in Europe[50] and to raise the relative cost of cloud service offerings.[51] Indeed, the above-referenced LSE study emphasized the role that misplaced governmental policies can and have already played in curtailing cloud computing industry growth in the European region. It concluded that, just as European governments' green energy policies have already raised the cost of energy to adversely impact cloud computing and related job growth in Europe, strict '[d]ata transfer policies, having to do with either trade or concerns such as data security and privacy rights protection, can have significant effect upon the economic dimensions of cloud computing. These can be directly translated into job effects.'[52]

EU governmental officials, however, do not appear to be heeding this advice, as may be discerned from the Working Party Opinion on Cloud Computing issued this past July by the independent European advisory body on data protection and privacy established pursuant to the EU Data Protection Directive.[53] While acknowledging 'the benefits of cloud computing in both economic and societal terms', the Opinion otherwise proceeds to reaffirm the application of existing and proposed EU data protection legislation to cloud computing. It accomplishes this by, once again, delineating for public bodies and private enterprises all of the data protection risks associated with 'wide scale deployment of cloud computing services', including cross-border data transfers outside the EU,[54] and by recommending due diligence steps that such parties 'should' take to reduce such risks contractually and through enforceable business compliance rules (BCRs), consistent with such legislation.[55]

6 Inconsistent national, regional regulatory frameworks retard cross-border cloud formations: 'adequacy' versus 'accountability' and related implications

It is significant that the OECD Guidelines and APEC Framework are each based on the principle of 'accountability'. Accountability is an organizationally focused approach that seeks to 'ensure that the original collector of the personal information remains accountable for compliance with the original privacy framework that applied when and where the data was collected, regardless of the other organisations or countries to which the personal data travels subsequently'.[56] APEC has recently taken the principle of cross-border 'accountability' to a new level vis-à-vis its recent development of a voluntary

Notes

4. Promote and enable the cross-border delivery of services; 5. Encourage multi-stakeholder co-operation in policy development processes; 6. Foster voluntarily developed codes of conduct; 7. Develop capacities to bring publicly available, reliable data into the policy-making process; 8. Ensure transparency, fair process, and accountability; 9. Strengthen consistency and effectiveness in privacy protection **at a global level**; 10. Maximise individual empowerment; 11. Promote creativity and innovation; 12. Limit Internet intermediary liability; 13. Encourage co-operation to promote Internet security; 14. Give appropriate priority to enforcement efforts.") (emphasis added).

47 See Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005) APEC website, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/—/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (accessed Aug. 23, 2012). Unlike the OECD Privacy Guidelines, the APEC Framework "does not explicitly state that there may or may not be national strengthening of its Principles, though this may be implied by some provisions." *See* Graham Greenleaf, *Five Years of the Apec Privacy Framework: Failure or Promise?*, 25 Computer Law & Security Report 28, 29 (2009), http://ssrn.com/abstract=2022907 (accessed Aug. 26, 2012).

48 *See* C. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* (2011), *supra* n. 18 at p. 14. *See also* OECD (2011), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, OECD Digital Economy Papers, No. 176, p.15 (OECD Publishing 2011), http://dx.doi.org/10.1787/5kgf09z90c31-enat , http://www.umic.pt/images/stories/publicacoes5/Privacy%20Guidelines.pdf.

49 *See* C. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* (2011), *supra* n. 18, at p. 17.

50 *See* Jeff Norman, *US to Europe: "Eat My Cloud Dust"*, CloudTweaks.com, http://www.cloudtweaks.com/2012/06/us-to-europe-eat-my-cloud-dust/(June 8, 2012).

51 *See* Deelip Menezes, *Will Cloud Computing Result In Uniform Pricing?*, Deelip.com, http://www.deelip.com/?p=7540(May 6, 2012). *See also* Kevin J. O'Brien, *Europe Turns to the Cloud*, N. Y. Times, http://www.nytimes.com/2011/07/25/technology/europe-turns-to-the-cloud.html?pagewanted=all (July 24, 2011).

52 *See* Jonathan Liebenau et al., *Modelling the Cloud: Employment Effects in Two Exemplary Sectors in the United States, the United Kingdom, Germany and Italy*, *supra* n. 26 at p. Executive Summary at p. 3, p. 61.

53 *See* Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing (01037/12/EN WP 196) (adopted July 1, 2012), accessible at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

54 *Id*., at pp. 4, 17–19.

55 *Id*., at Sec. 3.4.2 paras. 7, 14 pp. 13–14, Sec. 3.5.3 pp. 18–19.

56 *See* C. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* (2011), *supra* n. 18, at p. 14.

APEC Cross-Border Privacy Rules (CBPR) System.[57] The CBPR System, which is intended to assist APEC nations in implementing the APEC Framework, consists of four elements: (1) self-assessment; (2) compliance review; (3) recognition/acceptance; and (4) dispute resolution and enforcement.[58] 'Once an organization has been certified for participation in the CBPR System, CBPR program policies and practices will become binding as to that participant and will be enforceable by an appropriate authority, such as a regulator to ensure compliance with the CBPR program requirements.'[59]

The APEC Framework principle of accountability has been implemented at the national legislative level by the Government of Canada, as set forth in the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) which has been fully in force since 2004.[60] It is also contained within the *draft Privacy Principles* the Government of Australia released for public consultation in June 2010, as a preliminary response[61] to a 2008 Australian Law Reform Commission (ALRC) Report recommending changes to the *Australian Privacy Act*,[62] and within Section 16C of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* introduced in the Australian Parliament on 23 May 2012, implementing the Australian Government's response to ALRC Report recommendations.[63] The Canadian PIPEDA, for example, operates contrary to the 'state-to-state approach' adopted by the EU, and 'does not prohibit organisations in Canada from transferring personal information to an organization in another jurisdiction for processing.[64] However, under PIPEDA, organisations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement' by reference to national and contractual standards of responsibility to 'provide a comparable level of protection while the information is being processed by the third party'.[65] In other words, organizations must ensure, through contractual means or otherwise, a level of protection for personal information comparable to that available prior to its transfer.[66] Furthermore, recent Canadian case law reaffirms that cloud service providers will continue to be subject to PIPEDA when transmitting Canadians' personal information abroad to the US or other foreign office or to an affiliate or third party service provider.[67]

In stark contrast to the 'accountability' approach, stands the geographic 'adequacy' approach incorporated within Europe's 1995 Data Protection Directive. The 'adequacy' approach generally prohibits personal data transfers by organizations to jurisdictions geographically located outside the EU unless it is determined that the

Notes

[57] *See* Asia-Pacific Economic Cooperation, *APEC CBPR System — Policies, Rules and Guidelines*, 2011/SOM3/ECSG/DPS/009 at p. 2, http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_009.pdf (Sept. 18, 2011) (accessed Aug. 23, 2012).

[58] *See* Asia-Pacific Economic Cooperation, *APEC CBPR System – Policies, Rules and Guidelines*, *supra* n. 47 at par. 8, p. 4.

[59] *Id*.

[60] *See* Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data across Borders* (2009), at www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf (accessed Aug. 23, 2012).

[61] *See* Australian Government, *Australian Privacy Principles - Exposure Draft* (June 24, 2010) at pp. 15-17, www.smos.gov.au/media/2010/docs/Privacy-reform-exp-draft-part-1.pdf (accessed Aug. 26, 2010); Australian Government, *Australian Privacy Principles - Companion Guide* (June 2010), at pp. 13-14, www.smos.gov.au/media/2010/docs/100622-privacy-part-1-Companion-Guide.pdf (accessed Aug. 26, 2012). *See also* Christopher Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, supra at p. 17. The Exposure Draft was intended as a proposed legislative implementation of the Government of Australia's initial response to the ALRC Report. *See* Australian Government, *Enhancing National Policy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 - For Your Information: Australian Privacy Law and Practice* (Oct. 2009), available at: http://www.dpmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.pdf(accessed Aug. 26, 2012).

[62] *See* Australian Government, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice – Australian Law Reform Commission Report 108* , Vol. 2, Chap. 31 (May 2008), http://www.alrc.gov.au/sites/default/files/pdfs/publications/108_vol2.pdf (accessed Aug. 26, 2012).

[63] *See* The Parliament of the Commonwealth of Australia, House of Representatives, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012,* at Section 16C , at pp. 22, http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r4813_first-reps/toc_pdf/12080b01.pdf;fileType%3Dapplication%2Fpdf#search=%22legislation/bills/r4813_first-reps/0000%22; http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4813 (accessed Aug. 26, 2012) (implementing Australian Privacy Principle 8 (APP8) concerning cross-border disclosure of personal information). According to the explanatory memorandum accompanying the bill, "Section 16C is a key part of the Privacy Act's *new approach* to dealing with cross-border data flows. In general terms, there are currently two internationally accepted approaches to dealing with cross-border data flows: the adequacy approach, adopted by the European Union in the Data Protection Directive of 1996, and the accountability approach, adopted by the APEC Privacy Framework in 2004. NPP 9 was expressly based on the adequacy approach of the EU Directive. *Under the new reforms, APP 8 and section 16C will introduce an accountability approach more consistent with the APEC Privacy Framework*. The accountability concept in the APEC Privacy Framework is, in turn, derived from the accountability principle from the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 1980" (emphasis added). *See* The Parliament of the Commonwealth of Australia, House of Representatives, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012 Explanatory Memorandum* (2012), at p. 70, http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4813_ems_00948d06-092b-447e-9191-5706fdfa0728/upload_pdf/368711.pdf;fileType=application%2Fpdf (accessed Aug. 26, 2012). The bill was apparently subject to a second reading on August 23, 2012. *See* The Parliament of the Commonwealth of Australia, House of Representatives, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012 Second Reading Speeches* (Aug. 23, 2012), http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result/Second%20Reading%20Speeches.aspx?bId=r4813 (accessed Aug. 23, 2012).

[64] *See* Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data across Borders* (2009), at pp. 4–5, www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf.

[65] *Id.*

[66] *Id*.

[67] *See* Julio Arboleda Ramirez & Curtis Ellery Marble, *Canadian Privacy Law Goes Abroad – That's Data Protection!*, Alfa International, http://www.alfainternational.com/files/tbl_s12Publications/FileUpload92/271/Canadian%20Article.pdf; http://www.alfainternational.com/publications/pubs.aspx?view=all&pubtypeassetid=5003 (Mar. 2, 2010).

governments possess 'adequate legal or other data protection arrangements in place.[68] 'Currently, the adequacy of a third country – i.e., whether a third country ensures a level of protection that the EU considers as adequate – may be determined by the Commission and by Member States…However, the exact requirements for recognition of adequacy by the Commission are currently not specified in satisfactory detail in the Data Protection Directive', which has thereby led to 'different [non-uniform EU Member State Data Protection Authority] approaches to assessing the level of adequacy of third countries, or international organisations'.[69]

The current EU Data Protection Directive, which has been depicted by some in US academia as not being extra-territorial and as reflecting the weakness and inadequacy of American data privacy law,[70] has long been criticized. At least one legal commentator has described it as being over-inclusive, overbroad, unable to support the data protection structure, erroneously focusing on data as such (i.e., the collection and processing of data upstream), instead of harm arising from downstream data uses, seriously limiting valuable uses, and failing to balance competing interests properly (i.e., 'balancing the benefits of the free flow of information against the possible threats to privacy on a case-by-case basis').[71] In addition, the prior congressional testimonies of two former senior US officials reflected even deeper concerns about the EU Data Protection Directive. According to one such official, the Directive is: (i) reflective of Europe's particular legal and historical experience, 'including the police states and the holocaust'; (ii) 'often rigid or silent in dealing with privacy issues growing out of new technology and new business models' because it was conceived of at least twelve years before the Internet and the use of information-distributing networks, laptops and digital assistants; (iii) based on Europe's different conception of privacy as a human right obligation of the State toward its citizens, rather than as a right that inheres in the individual that can be traded if desired; and iv) potentially disruptive of international and transatlantic commerce primarily because it 'would embargo European personal data to any country . . . including the United States . . . whose privacy policies . . . the EU had not approved'.[72] The second such official emphasized that the Directive: (i) has 'extraterritorial impact' because it 'regulates cyber space and much offline activity as well'; (ii) has encouraged other countries to adopt 'privacy laws, some of which, including Canada's, have substantial potential extraterritorial impact', and consequently, has led to 'a maze of conflicting provisions that create a complex, perilous, and potentially non-navigable environment for the many firms that process personal data which crosses borders'; (iii) could potentially 'regulate substantial amounts of data processing within the United States', and thereby 'place at risk U.S. competitiveness, U.S. trade, and fundamental U.S. values, including rights protected under the First Amendment'; (iv) is 'tantamount to extortion' to the extent it requires all other countries to 'adopt . . . EU . . . privacy laws or risk having data flows to them cutoff by all of the EU's Member States'; and (v) 'threatens national sovereignty [to the extent the] EU . . . insist[s] that it be treated as the de facto global standard for privacy'.[73] More recently, the cloud computing industry expressed its concern that the Directive's 'registration requirements for data controllers or data transfers may act as barriers to the take-up of cloud services'.[74]

These criticisms reflected US government and industry frustration with the economic, legal and political impact of the EU's unilateral determination that the US system was not 'adequate' for protecting the privacy of EU citizens. They were expressed during congressional hearings held to review the effectiveness of the EU–US safe harbour agreement subsequently negotiated in response to such determination, which was scheduled to expire during 2001. As the testimony of one such former official reveals, the safe harbour was less than sufficient to protect US interests and was of limited utility because it

Notes

[68] *See* OECD (2011), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, *supra* n. 48 at p. 32; Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, *supra* n. 44 at pp. 2024, 2027.

[69] *See* European Commission, *A Comprehensive Approach On Personal Data Protection in the European Union*, *supra* n. 39 at Sec. 2.4.1, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

[70] *See Statement of Joel R. Reidenberg, Professor of Law, Fordham University School of Law*, The EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce, House of Representatives, 107th Congress, 1st Session, Mar. 8, 2001 (Serial No. 107–19), at pp. 66–67 http://republicans.energycommerce.house.gov/107/action/107-19.pdf.

[71] *See e.g.,* Lucas Bergkamp, *EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 Computer Law & Security Review 31, 42 (January 2002) http://www.hunton.com/files/Publication/cfd01362-a4c2-42b9-a617-c83082a289d7/Presentation/PublicationAttachment/891e6ada-3402-44d1-b1f7-b40c8f3af95a/Privacy_fallacy.pdf; http://www.sciencedirect.com/science/article/pii/S0267364902001061.

[72] *See Statement of David L. Aaron, Senior International Advisor, Dorsey & Whitney LLP, former Undersecretary of Commerce for International Trade*, The EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce, House of Representatives, 107th Congress, 1st Session, Mar. 8, 2001 (Serial No. 107–19), *supra* n. 64 at p. 42.

[73] *See Statement of Jonathan M. Winer, Counsel, Alston and Byrd LLP, former U.S. Deputy Assistant Secretary of State for International Law Enforcement*, The EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce, House of Representatives, 107th Congress, 1st Session, Mar. 8, 2001 (Serial No. 107–19), *supra* n. 64 at pp. 45–47.

[74] *See* Business Software Alliance, *BSA Global Cloud Computing Scorecard 2012*, at p. 4, http://portal.bsa.org/cloudscorecard2012/; http://portal.bsa.org/cloudscorecard2012/assets/PDFs/BSA_GlobalCloudScorecard.pdf.

'exclude[ed] the most important sectors of the U.S. economy, including telecommunications as well as financial services'.[75] Canada, by contrast, was included 'among the nine countries that [the EU] . . . recognized . . . [as] . . . "ensur[ing] an adequate level of protection"', because the EU Commission had determined that PIPEDA provided an adequate level of protection for personal data transferred from the European Community to recipients in Canada.[76] The EU did not, however, lavish the data protection regimes of India, China or Japan with the same high regard. India has not yet received a response from the EU to its October 2009 request for an adequacy assessment,[77] while neither China nor Japan has yet 'been the subject of a formal EU adequacy decision [, which] means that there must be substantial non-compliance at least with regard to data flows from the EU to those countries'.[78]

The Madrid Resolution,[79] adopted during November 2009 at the International Conference of Data Protection and Privacy Commissioners, represents 'the most recent effort to develop international data privacy principles'.[80] It sets forth principles that are 'broadly similar to the framework of the EU Directive, except that they are nonbinding'.[81] For example, Resolution paragraph 15.1 provides that 'international transfers of personal data may be carried out when the State to which such data are transmitted affords, as a minimum, the level of protection provided for in the' Resolution.[82] Resolution paragraph 15.2 provides that 'international transfers of personal data to States that do not afford the level of protection provided for in this' Resolution may be carried out if 'those who expect to transmit such data guarantee that the recipient will afford such level of protection'. This can be achieved by means of 'appropriate contractual clauses', or 'where the transfer is carried out within corporations or multinational groups, such guarantees may be contained in internal privacy rules, compliance with which is mandatory'.[83] Resolution paragraph 15.3 provides that States may permit the 'international transfer of personal data to [other] States that do not afford the level of protection provided for in this [Resolution], where necessary and in the interest of the data subject in the framework of a contractual relationship, to protect the vital interests of the data subject or of another person, or when legally required on important public interest grounds',[84] as similarly contemplated within the exceptions to EU Directive Article 26(1).[85] Lastly, Resolution paragraph 15.4 empowers State data supervisory authorities, consistent with Resolution paragraph 23, to authorize some or all of the international transfers falling within their jurisdiction, before they are carried out.[86] Commentators believe that the ultimate goal of the fifty countries that introduced the Madrid Resolution is 'to make the principles binding on the Resolution's signatories'.[87]

In fact, the EU Commission's recent proposal for an EU-wide General Data Protection Regulation (the 'Proposed Regulation')[88] was inspired by the Madrid Resolution.[89] The Proposed Regulation's aim is to significantly reduce the legal and economic uncertainty inherent in the design and application of the current EU Data Protection Directive. It also appears to go beyond existing voluntary and regulatory regimes by embracing a combined 'organisationally-based approach[] that allow[s] geography to be considered in making decisions about whether the transfer of personal data abroad is

Notes

[75] *See Statement of Jonathan M. Winer, Counsel, Alston and Byrd LLP, former U.S. Deputy Assistant Secretary of State for International Law Enforcement*, *supra* n. 67 at p. 46. *See also Prepared Statement of Jonathan M. Winer, Counsel, Alston and Byrd LLP, former U.S. Deputy Assistant Secretary of State for International Law Enforcement*, *supra* at p. 50.

[76] *See* Article 1, *Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Canadian Personal Information Protection and Electronic Documents Act*, 2002/2/EC, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:002:0013:0016:EN:PDF.

[77] *See* Graham Greenleaf, *India's U-Turns on Data Privacy*, Berkeley Electronic Press Paper 45 (2011), at p. 19, http://law.bepress.com/cgi/viewcontent.cgi?article=1314&context=unswwps.

[78] *See also* C. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* (2011) *supra* n. 18 at p. 21.

[79] *See International Standards on the Protection of Personal Data and Privacy – The Madrid Resolution*, (The Resolution) International Conference of Data Protection and Privacy Commissioners, http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf (Nov. 5, 2009).

[80] *See also* C. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* (2011) *supra* n. 18 at p. 20.

[81] *Id*.

[82] *See* Madrid Resolution, *supra* n. 73 at par. 15.1

[83] *See* Madrid Resolution, *supra* n. 73 at par. 15.2.

[84] *See* Madrid Resolution, *supra* n. 73 at par. 15.3.

[85] *See also* C. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* (2011) *supra* n. 18 at p. 19.

[86] *See* Madrid Resolution, *supra* n. 73 at paras. 15.4, 23.

[87] *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n. 12 at p. 16, citing 31st International Conference of Data Protection and Privacy (ICDPP), *Data Protection Authorities from over 50 Countries Approve the Madrid Resolution* (November 2009), ICDPP Press Release http://www.gov.im/lib/docs/odps//madridresolutionpressreleasenov0.pdf.

[88] See *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final (1/25/2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[89] *See* General Data Protection Regulation, *supra* n. 82 at Explanatory Memorandum Section 3.4.3.1.

appropriate', in line with prior OECD recommendations.[90] Pursuant to Article 41 of the Proposed Regulation, digital transfers by controllers or processors of personal data outside the EU to third countries would be subject to an 'adequacy' procedure that expressly permits the EU Commission to consider[91] the state of third country or international rule of law and judicial redress, the effective functioning of third country or international organization independent supervisory authorities, and the international commitments to which such third countries and international organizations are bound.[92] Where the EU Commission has not adopted an adequacy decision, proposed Article 42 would require a data controller or processor to 'adduce . . . appropriate safeguards with respect to the protection of personal data in a legally binding instrument'.[93] This can be accomplished, on the one hand, via reference to binding corporate rules or standard EU Commission-adopted data protection clauses.[94] On the other hand, this can be achieved by referring to standard data protection clauses adopted consistently by, or privately negotiated contractual clauses (i.e., negotiated between cloud service providers (controllers or processors) and data recipients) authorized by,[95] newly established EU Member State independent supervisory authorities.[96] Such authorities are also to be empowered, individually and jointly, to 'hear and investigat[e] complaints and [to] promot[e] the awareness of the public of risks, rules, safeguards and rights',[97] among other tasks.[98] Criticism of the EU Commission's preferred version of the Proposed Regulation began shortly after its release.[99] At least one legal commentator has observed that its provisions are overly legalistic, difficult and costly to implement in practice (especially by SMEs), not reflective of basic differences in legal systems and administrative cultures that are not likely susceptible to harmonization with Brussels, excessively punitive, insufficiently aware of 'the realities of massive international data transfers via phenomena such as cloud computing', and potentially indicative of trade protectionist design and effect.[100]

Besides the aforementioned data privacy/protection regimes, the governments of India,[101] Japan,[102] Malaysia,[103] the Philippines,[104] Singapore,[105] South Korea[106] and Taiwan[107] have also adopted or proposed their own regulations some of which are influenced by the EU Data Protection Directive. These measures, which are informed largely by legal and cultural tradition, are sufficiently different from (and inconsistent with) one

Notes

[90] *See* C. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* (2011), *supra* n. 18 at p. 8.

[91] *See* General Data Protection Regulation, *supra* at Explanatory Memorandum Section 3.4.5 p. 11, Article 41(1).

[92] *Id*., at General Data Protection Regulation Articles 41(2)(a)-(c), 41(3), 41(5).

[93] *Id*., at General Data Protection Regulation Article 42(1).

[94] *Id*., at General Data Protection Regulation Article 42(2)(a)-(b).

[95] *Id*., at General Data Protection Regulation Articles 42(2)(c)-(d), 56–57; Sections 3.4.5–3.4.6, pp. 11–12.

[96] *Id*., at General Data Protection Regulation Articles 46–47; Sec. 3.4.6, p. 12.

[97] *Id*., at General Data Protection Regulation Articles 52(1)(b)-(d), (f); Sec. 3.4.6, p. 12.

[98] *Id*., at General Data Protection Regulation Articles 53, 56-57.

[99] *See CBI Joins Criticism of EU Data Law*, DecisionMarketing.com, http://www.decisionmarketing.co.uk/?p=9364 (Mar. 19, 2012); New EU Data Laws 'to Cost Millions', DecisionMarketing.com, http://www.decisionmarketing.co.uk/?p=9306 (Mar. 15, 2012); Stuart Sumner, *Analysis: Data Protection – Is the EU Going Too Far?*, Computing.co.uk, http://www.computing.co.uk/ctg/analysis/2144279/analysis-protection-eu (Feb. 6, 2012); *EU Proposed Data Protection Overhall; Criticism Ensues*, SimplySecurity.com, http://www.simplysecurity.com/2012/02/03/eu-proposes-data-protection-overhaul-criticism-ensues/ (Feb. 3, 2012); Bart Porter, *EU Proposed Data Security Regulations Stir Debate, Controversy Around the Globe*, (re)Blog, http://blog.redemtech.com/2012/02/eu-proposed-data-security-regulations-stir-debate-controversy-around-the-globe.html (Feb. 2, 2012); Grant Gross, *Critics: EU's Proposed Data Protection Rules Could Hinder Internet*, PC World Australia, http://www.pcworld.idg.com.au/article/413430/critics_eu_proposed_data_protection_rules_could_hinder_internet/ and http://www.pcworld.com/businesscenter/article/248732/critics_eus_proposed_data_protection_rules_could_hinder_internet.html (Jan. 26, 2012).

[100] *See* Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, Bloomberg BNA Privacy and Security Law Report (11 PVLR 06, 02/06/2012) at pp. 14-15, http://www.huntonprivacyblog.com/wp-content/uploads/2012/02/Kuner-EU-regulation-article.pdf. *See also* SEC(2012) 72 final at p. 89; SEC(2012) 73 final at p. 9. *See also* Cornelius Rahn, *Europe Won't Let U.S. Dominate Cloud With Rules to Curb HP: Tech*, Bloomberg News, http://www.bloomberg.com/news/2012-01-17/europe-won-t-let-u-s-dominate-cloud-with-rules-to-curb-hp-tech.html (Jan. 17, 2012).

[101] *See* Graham Greenleaf, *India's U-Turns on Data Privacy*, *supra* n. 71 at pp. 3–4, 10.

[102] *See* ZL Technologies, Inc., *Regulation Overview: Japan's Personal Information Protection Act (PIPA)* (2005), http://www.zlti.com/content/docs/Rules%20and%20Regulations/ZLRR.Japan-PIPA.pdf. *See also* Yukiko Ko, *Japan at The Critical Juncture on Data Protection: Personal Information Protection Act and Its Guidelines Under Review*, BNA Privacy & Security Law Report (Vol. 5, No. 49, 12/18/2006), at p.4, http://www.alston.com/files/Publication/62f79d71-e594-49af-ace2-379b14db302c/Presentation/PublicationAttachment/8ab60ac2-5b8a-4aaf-91ea-13c3403242f7/KoBNAJapanDataProtection.pdf.

[103] *See* Graham Greenleaf, *ASEAN's 'New' Data Privacy Laws: Malaysia, the Philippines and Singapore*, Berkeley Electronic Press Paper 14 (2012), at p. 1, http://law.bepress.com/cgi/viewcontent.cgi?article=1346&context=unswwps.

[104] *Id*., at pp. 2–3.

[105] *Id*., at p. 4.

[106] *See* Hunton & Williams, LLP, *Korea Announces Regulations to Personal Information Protection Act*, Privacy and Information Security Law Blog, http://www.huntonprivacyblog.com/2011/06/articles/korea-announces-regulations-to-personal-information-protection-act/(June 2, 2011). *See also* Kwang Hyun Ryoo & Ji Yeon Park, *Further Korean Data Privacy Rules Announced*, BKL Legal Update, at p. 2, http://www.bkl.co.kr/kor/_common/filedownload.asp?file=doc\bkl-koreanlawupdate-20110531.pdf (May 31, 2011).

[107] *See* H. Henry Chang & Chris H.C. Tsai, *Taiwan's New Personal Data Protection Law*, Baker & McKenzie, http://www.bakermckenzie.com/RRTaiwanPersonalDataProtectionLawOct10/(October 2010).

another to raise considerable uncertainties and tensions among cloud computing providers with respect to cross-border data transfers.[108] Unfortunately, such rules also ignore the reality of cloud computing which (like corporate groups and online business) reduces physical borders to technical irrelevance.[109]

Notwithstanding the potential of cross-border cloud computing to stimulate innovation and economic growth, the prolific pace at which governments have introduced new national data privacy/protection initiatives strongly 'suggest[s] that the "free flow of information" is becoming more conditional and that enterprises will have to be nimble to meet the expectations of regulators, consumers, and employees when the organization wants to move personally identifiable data from one country to another'.[110] In fact, transborder data flow regulation is already playing 'a significant role in business decisions', including those relating to where, when and if particular international personal data transfers and processing activities will be undertaken.[111]

7 The risk of trade protectionism grows in the absence of binding and coherent international rules governing cross-border cloud computing services

Precisely because the restrictive emerging rules 'governing the provision of digital commercial financial services, technology products or the treatment of information' increasingly appear 'to favor domestic interests over international competition' the US-based National Foreign Trade Council (NFTC) recently alleged that digital protectionism has become 'a growing threat around the world',[112] an observation that has also been registered by the Business Software Alliance (BSA) in its recently released 'cloud computing scorecard'.[113] To reduce such risk, the NFTC has called upon the US government, at various international venues, 'including the World Trade Organization (WTO), APEC forum, OECD', and the ongoing Trans-Pacific Partnership regional trade negotiations, to 'drive the development and adoption of transparent and high-quality international rules, norms and best practices on cross-border flows of digital data and technologies while also holding countries to existing international obligations'.[114]

The ability of the US government to hold countries to existing WTO obligations, however, will likely prove quite challenging. WTO Members have, on several occasions, endeavoured to review and renegotiate[115] the WTO Information Technology Agreement (ITA)[116] for purposes of expanding its coverage.[117] However, since the ITA's scope of coverage is limited specifically to products (equipment),[118] it does not include transformative ICT services such as cloud computing[119] which has essentially 'centralized many of the functionalities in today's goods and turn[ed] them into online services'.[120] According to at least one commentator, '[d]igital products have been of major concern since a delivery is possible by means of physical data carrier or by electronic transfer. If a disk is used, the regulatory framework of the ITA is applicable to

Notes

[108] *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n. 12 at p. 13, *citing* United States Department of Commerce, *Selected Asia and Oceania Data Protection Laws*, http://web.ita.doc.gov/ITI/itiHome.nsf/0657865ce57c168185256cdb007a1f3a/75a970b3ad293d788525773c0071233c/$FILE/Selected%20Asia%20and%20Oceania%20Data%20Protection%20Laws%206-11.pdf (June 2011). *See also* Graham Greenleaf, *ASEAN's 'New' Data Privacy Laws: Malaysia, the Philippines and Singapore*, *supra* n. 97 at p. 1.

[109] *See* W. Scott Blackmer, *Transborder Data Flows at Risk*, InfoSecisland.com, http://www.infosecisland.com/blogview/20585-Transborder-Data-Flows-at-Risk.html (Mar. 22, 2012).

[110] *Id*.

[111] *See also* C. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* (2011), *supra* n. 18 at p. 21.

[112] *See* National Foreign Trade Council, *Promoting Cross-Border Data Flows: Priorities for the Business Community*, at p. 1, http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf (November 2011).

[113] *See* Business Software Alliance, *BSA Global Cloud Computing Scorecard 2012*, *supra* n. 68 at p. 6.

[114] *Id*.

[115] *See* World Trade Organization, *EU Pushes for Review of Information Technology Agreement*, WTO 2010 News Items, http://www.wto.org/english/news_e/news10_e/ita_11nov10_e.htm (Nov. 11, 2010). *See also* Hosuk Lee-Makiyama, *Future-Proofing World Trade in Technology: Turning the WTO IT Agreement (ITA) into the International Digital Economy Agreement (IDEA)*, European Centre for International Political Economy (ECIPE) Working Paper No. 04/2011 (2011), at p. 4, http://www.ecipe.org/media/publication_pdfs/WP201104.pdf.

[116] *See* World Trade Organization, *Ministerial Declaration on Trade in Information Technology Products*, (WT/MIN(96)/16), http://www.wto.org/english/docs_e/legal_e/itadec_e.pdf (Dec. 13, 1996). *See also* Hosuk Lee-Makiyama, *Future-Proofing World Trade in Technology: Turning the WTO IT Agreement (ITA) into the International Digital Economy Agreement (IDEA)*, *supra* n. 109 at p. 3.

[117] *See* World Trade Organization, *Informal Talks Set to Begin On Expanding the Information Technology Agreement*, WTO 2012 News Items, http://www.wto.org/english/news_e/news12_e/ita_15may12_e.htm (May 15, 2012); World Trade Organization Committee of Participants on the Expansion of Trade in Information Technology Products, *Concept Paper for the Expansion of the ITA*, Communication from Canada, Japan, Korea, the Separate Customs Territory of Taiwan, Penghu, Kinmen and Matsu, Singapore and the United States, (G/IT/W/36), accessible at: www.wtocenter.org.tw/SmartKMS/fileviewer?id=124962 (May 2, 2012).

[118] *Id*. ITA Appendices A and B cover a number of products, including: semiconductors, semiconductor manufacturing and testing equipment, computers, flat panel displays, computer network equipment, computer software, telecommunication products and scientific instruments.

[119] *See* Hosuk Lee-Makiyama, *Future-Proofing World Trade in Technology: Turning the WTO IT Agreement (ITA) into the International Digital Economy Agreement (IDEA)*, *supra* n. 109 at p. 5.

[120] *Id*., at p. 18.

the extent that this carrier medium is listed in Appendices A or B; in case of an electronic transmission, the GATS rule would apply.'[121] Furthermore, the definition of 'computer and related services' (CRS) to which theeighty-three WTO Member parties of the WTO General Agreement on Trade in Services (GATS)[122] have made commitments is outdated,[123] and '[t]here [still] is no consensus about the extent to which this definition applies to cloud computing activities' other than data processing.[124] While the US and 'several other members previously submitted a proposal in 2007 that would define ["computer and related services"] as covering "all computer and related services…regardless of whether they are delivered via a network, including the Internet"',[125] said proposal has not yet been approved (i.e., as of May 2012).[126] In addition, although some of the activities defined as 'value-added' telecommunication services within the GATS Annex on Telecommunications[127] 'may overlap with cloud computing' in light of the voluntary commitments made by sixty WTO members with respect to 'on-line information and/or data processing',[128] WTO members have yet to agree that such annex expressly and clearly applies to other cloud characteristics.

It is perhaps for these reasons that at least one European think-tank (ECIPE) has recommended that WTO Members seek to reform (broaden and deepen) the scope of the ITA[129] by, among other means, extending coverage to network-based services that are compatible with emerging ICT product technical standards and without which the newest of ICT products could no longer largely function.[130] According to ECIPE, 'developments in cloud computing will centralize many of the functionalities in today's goods and turn them into online services. A substantial part of the ICT industry's value added, that comes from technical infrastructure, platforms and software, is increasingly provided as services on a global basis'.[131] The NFTC, as well, has called upon the US government to 'pursue ad hoc or informal…bilateral or multilateral…frameworks to clarify rules and standards and improve transparency…[as] where regimes take divergent approaches to complex issues such as privacy or government access to data…[Such frameworks]…could be designed to address key issues, such as clarifying jurisdiction over data or bridging national privacy regimes'.[132]

In this regard, commentators have cited the US–Korea Free Trade Agreement (KORUS FTA),[133] which entered into force on 15 March 2012, as a high standard to emulate because it 'contains more provisions relating to the cloud than previous U.S. trade agreements'.[134] The KORUS FTA's focus on cloud computing is apparently linked to the potential competition that US-based cloud providers are facing in the Korean market due to 'Korea's global leadership [position] in wireless

Notes

[121] *See* Rolf H. Weber, *Digital Trade in WTO-Law - Taking Stock and Looking Ahead*, 5 Asian J. WTO & Intl Health L. & Policy 1, 8, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1578139&download=yes (March 2010).

[122] *See* General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, THE LEGAL TEXTS: THE RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS 284 (1999), 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994), http://www.wto.org/english/docs_e/legal_e/26-gats.pdf.

[123] *See* United Nations, *Provisional Central Product Classification (Provisional CPC), Chapter 84 – Computer and Related Services* (1990), http://unstats.un.org/unsd/cr/registry/regcs.asp?Cl=9&Lg=1&Co=84 ; http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=9&Lg=1; United Nations Department of Economic and Social Affairs Statistics Division, *Central Product Classification (CPC) Version 1.1*, Statistical Paper Series No. 77 Ver. 1.1 (2002), at p. 422, http://unstats.un.org/unsd/publication/SeriesM/SeriesM_77ver1_1E.pdf.

[124] *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n. 12 at p. 21.

[125] *See* World Trade Organization, *On the Understanding on the Scope of Coverage of CPC 84 - Computer and Related Services*, Communication from Albania, Australia, Canada, Chile, Colombia, Croatia, the European Communities, Hong Kong China, Japan, Mexico, Norway, Peru, the Separate Customs Territory of Taiwan Penghu, Kinmen and Matsu, Turkey and the United States to the Council for Trade in Services (TN/S/W/60 & S/CSC/W/51), http://trade.ec.europa.eu/doclib/docs/2008/september/tradoc_140348.pdf (Jan. 26, 2007).

[126] *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n. 12 at p. 21.

[127] *See* World Trade Organization, *TELECOMMUNICATIONS SERVICES: ANNEX - Explanation of the Annex on Telecommunications*, WTO website, http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_annex_expl_e.htm (The GATS Annex on Telecommunications 'requires each Member to ensure that all service suppliers seeking to take advantage of scheduled commitments are accorded access to and use of public basic telecommunications, both networks and services, on reasonable and non-discriminatory basis').

[128] *Id.,* at pp. 21–22. *See also* World Trade Organization Council for Trade in Services, *Telecommunication Services – Background Note by Secretariat*, (S/C/W/299) at par. 7, and Figure A1- Telecommunications services in the GATS Services Sectoral Classification List (MTN/GNS/W/120) at p. 20 ('Value-added' telecommunication services include those falling 'within subsectors h. through n'… 'h. Electronic mail 7523; i. Voice mail 7523; j. On-line information and data base retrieval 7523; k. electronic data interchange (EDI); l. enhanced/value-added facsimile services, incl. store and forward, store and retrieve 7523; m. code and protocol conversion n.a.; n. on-line information and/or data processing (incl.transaction processing) 843').

[129] *See also* Hosuk Lee-Makiyama, *Future-Proofing World Trade in Technology: Turning the WTO IT Agreement (ITA) into the International Digital Economy Agreement (IDEA)*, *supra* n. 109 at pp. 6–7, 11, 17–22.

[130] *Id*., at p. 17.

[131] *Id*., at p. 18.

[132] *See* National Foreign Trade Council, *Promoting Cross-Border Data Flows: Priorities for the Business Community*, *supra* n. 106 at p. 6.

[133] *See* Office of the United States Trade Representative, *Free Trade Agreement Between the United States of America and the Republic of Korea*, http://www.ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text.

[134] *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n. 12 at p. 22.

communicationsand broadband Internet access services',[135] and toemerging trends 'in the Korean software services market…driven by cloud computing as part of software application services'.[136] For example, Article 15.8 (Cross-Border Information Flows) provides that, 'Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.'[137] Although the language of such article may appear hortatory and non-binding,[138] it is circumscribed by three well-established binding WTO principles,[139] namely, those of national treatment and most favoured nation (MFN) status[140] and no unnecessary obstacles to trade in products[141] and services.[141]

Moreover, commentators have also pointed to the ongoing Trans-Pacific Partnership Agreement (TPP) negotiations as providing an important venue within which national and regional governments might cooperatively work to establish an international 'gold' standard that promotes cross-border data flows that can enhance the growth of cloud computing and other emerging digital technologies within the dynamic Asia-Pacific rim. The TPP is an Asia-Pacific regional (plurilateral) trade agreement first negotiated between Brunei, Chile, New Zealand, and Singapore during 2002–2005. It was subsequently signed by each nation during 2005,[143] and later went into effect on 8 November 2006.[144] This original (P4) group was subsequently expanded to include Australia, Peru and the US which joined in 2008,[145] Malaysia and Vietnam which joined in 2010,[146] and Canada and Mexico which joined in 2012.[147] Although both Japan and South Korea have been invited, neither has yet decided whether to join TPP negotiations.[148]

The NFTC, a recognized free trade advocate and cloud computing industry supporter, has referred to the emerging Trans-Pacific Partnership Agreement (TPP) as providing an 'ideal opportunit[y] to leverage and build on existing commitments that already address cross-border flows for the financial services sector'.[149] In particular, the NFTC seeks for negotiators to introduce new language that expressly permits cross-border information flows for other sectors, and prohibits the linking of market access or other commercial benefits to the satisfaction of 'localization' requirements – that is, rules that require providers of computer or data processing services to locate (invest in or establish) their facilities 'locally'.[150] Similarly, the Business Roundtable has called for the US government to propose as binding policy for adoption by all TPP negotiating members: i) the implementation of 'the E.U.-

Notes

[135] *See* United States Department of Commerce, U.S. Commercial Service, *Doing Business in Korea: 2011 Country Commercial Guide for US Companies* (2011), at p. 31, http://www.mac.doc.gov/japan-korea/nte/2011ccg-korea.pdf.

[136] *Id*.

[137] *See* Office of the United States Trade Representative, *Korean-United States Free Trade Agreement, Chapter 15 – Electronic Commerce* (2011), http://www.ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf.

[138] *See* Louis Antonacci, *Lessons from LaGrand: An Argument for the Domestic Enforceability of Treaty-Based Rights Under International Prisoner Transfer Treaties*, 3 Santa Clara J. Intl. L. 22, 43 (2005), http://digitalcommons.law.scu.edu/scujil/vol3/iss1/2, citing *Sale v. Haitian Centers Council, Inc.*, 113 S. Ct. 2549 (1993) at 2551-52. *See also* Juscelino F. Colares, *A Theory of WTO Adjudication: From Empirical Analysis to Biased Rule Development*, 42 Vand. J. Transnatl. L. 383, 424–427 (2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1363912.

[139] *See* Renee Berry & Matthew Reisman, *Policy Challenges of Cross-Border Cloud Computing*, *supra* n. 12 at p. 22.

[140] *See* Office of the United States Trade Representative, *Free Trade Agreement Between the United States of America and the Republic of Korea*, *supra* n. 127 Articles 2.2, 2.3.

[141] *Id.,* Article 9.1.

[142] *Id.,* Article 12.7.2.

[143] *See Trans-Pacific Partnership Agreement*, as entered into force on Nov. 8, 2006, www.sice.oas.org/Trade/CHL_Asia_e/mainAgreemt_e.pdf.

[144] *See Trans-Pacific Strategic Economic Partnership Agreement (P4), Chile-Brunei Darussalam-New Zealand-Singapore, Foreign Trade Information System*, Organization of American States, www.sice.oas.org/TPD/CHL_Asia/CHL_Asia_e.ASP.

[145] *See* The Hon Simon Crean MP Former Minister for Trade, *Australia to Join Efforts to Promote Free Trade in Asia Pacific*, Ministerial Statement: The Trans Pacific Partnership, http://trademinister.gov.au/speeches/2008/081126_tpp.html (Nov. 26, 2008); Trans-Pacific Partnership Digest, *TPP Background*, http://tppdigest.org/index.php?option=com_content&view=section&layout=blog&id=5&Itemid=53; Ian F. Fergusson & Bruce Vaughn, *The Trans-Pacific Partnership Agreement*, Congressional Research Service (CRS) Report for Congress R40502 at p. 1, http://fpc.state.gov/documents/organization/145583.pdf (June 25, 2010) ('In March 2008, the United States joined the [Tpp] negotiations to conclude the investment and financial services provisions').

[146] *See* Government of Malaysia Ministry of International Trade and Industry, *Malaysia Joins the Trans-Pacific Partnership Agreement Negotiations*, Media Release, http://www.miti.gov.my/cms/content.jsp?id=com.tms.cms.article.Article_86fa2f4c-c0a81573-f5a0f5a0-94e78b70 (Oct. 6, 2010); *Nation Joins Trans-Pacific Partnership*, VietNamNet Bridge, http://english.vietnamnet.vn/en/politics/1488/nation-joins-trans-pacific-partnership.html (Nov. 15, 2010).

[147] *See* Louise Egan, *Canada to Join Trans-Pacific trade Talks*, Reuters, http://www.reuters.com/article/2012/06/19/us-g20-canada-tpp-harper-idUSBRE85I1AL20120619 (June 19, 2012); Doug Palmer, *Mexico to Join Trans-Pacific Partnership Talks*, Reuters, http://www.reuters.com/article/2012/06/18/us-usa-mexico-transpacific-idUSBRE85H1LC20120618 (June 18, 2012).

[148] *See* Jonathan Manthorpe, Trans-Pacific Partnership Viewed with Skepticism, The Vancouver Sun, http://www.vancouversun.com/business/Trans+Pacific+Partnership+viewed+with+skepticism/6835111/story.html (June 25, 2012); *Japan Should Speed Up Efforts to Join TPP Negotiations*, The Yomiuri Shimbun, http://www.yomiuri.co.jp/dy/editorial/T120622003596.htm (June 23, 2012); *South Korea Prioritizes Asia Trade Pacts Over Pacific Partnership*, Reuters, http://ajw.asahi.com/article/behind_news/politics/AJ201205170023 (May 17, 2012).

[149] *See* National Foreign Trade Council, *Promoting Cross-Border Data Flows: Priorities for the Business Community*, *supra* n. 106 at p. 5.

[150] *Id* (The NFTC also seeks new language that improves transparency, IPR systems, ICT market access, and cooperation on ICT standards and conformity assessment).

U.S. Trade Principles for Information and Communication Technology Services[151] and the OECD Principles for Internet Policy-Making[152] – particularly the rules governing the location of infrastructure for cross-border data services'; and (ii) an agreement 'not [to] impose blanket local data server requirements except when necessary to protect against genuine national security risks', and 'only after fully considering alternative solutions through consultation and collaboration with the business community and only if such alternatives would be ineffective in addressing the genuine national security concern'.[153]

To this end, the US government recently submitted a proposal to be included in the TPP's e-commerce chapter that:

> foresees binding, enforceable language obligating TPP countries not to block the cross-border transfer of data over the Internet. It also includes a binding obligation that a TPP country cannot require a company to locate its data servers in its territory as a condition of doing business there…The data flow proposal is something that the U.S. has never before attempted in a trade agreement.[154]

However, during the TPP's May 2012 negotiating round that took place in Dallas, Texas, the US proposal faced objections from the governments of Australia and New Zealand because of its potential to conflict with their privacy laws. Australia was reported to be reluctant to fully support the proposal following its May 2012 announcement that it would reform national privacy laws 'to better protect people's personal information', which amendment was subsequently introduced by the Australian Parliament on 23 May 2012.[155] Meanwhile, New Zealand was reported to question 'whether the U.S. proposal could force a country to transmit or locate the data in another TPP country where it would be subject to laws that could breach the privacy of its citizens…[i.e.,] the Patriot Act', and whether it 'would infringe on [New Zealand's] right to require a company to keep user data in local servers'.[156]

Perhaps, the difficulties the US government has encountered in gaining international support for its proposal at TPP negotiations are, in part, attributable to the perceived inconsistency between the national security concern-based localization requirements imposed by the US federal government with respect to government procurement-related cloud computing services, and the voluntary consumer privacy framework promoted by the U.S. government with respect to private party cloud computing service arrangements which do not impose localization requirements. On the one hand, the US government's Federal Cloud Computing Strategy imposes obligations on federal agencies 'to ensure that a safe, secure cloud solution is available to provide a prospective IT service, and should carefully consider agency security needs across a number of dimensions, including but not limited to…[d]ata controls and access policies to determine where data can be stored and who can access physical locations'.[157] Such national security concerns were discussed at specially convened congressional hearings during October 2011,[158] and were emphasized in the Business Roundtable's recent report.[159] Apparently, US Government cloud computing-related national security concerns have also given rise to federal agency cloud computing contract language limiting data centre locations for national security reasons.[160] On the other hand, the Consumer Privacy Bill of Rights unveiled by the

Notes

[151] *See European Union-United States Trade Principles for Information and Communication Technology Services* (adopted Apr. 4, 2011), at paras. 3–4, accessible at: http://www.ustr.gov/webfm_send/2780.

[152] *See* Organization for Economic Cooperation and Development, *OECD Council Recommendation on Principles for Internet Policy Making*, at p. 7, http://www.oecd.org/dataoecd/11/58/49258588.pdf (Dec. 13, 2011).

[153] *See* Business Roundtable, *Promoting Economic Growth Through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements* at p. 9, http://businessroundtable.org/uploads/studies-reports/downloads/Global_IT_Policy_Paper_final.pdf (June 2012).

[154] *See U.S. Cross-Border Data Flow Proposal Raises Privacy Questions*, Insidetrade.com, http://insidetrade.com/201205152398886/WTO-Daily-News/Daily-News/us-cross-border-data-flow-proposal-raises-privacy-questions/menu-id-948.html; http://pastebin.com/cgtWYEc1 (May 12, 2012). *See also* William J. Weber, *Privacy Across Borders: Concerns Surfacing in Trans-Pacific Partnership*, Data Privacy Monitor, http://www.dataprivacymonitor.com/international-privacy-law/privacy-across-borders-concerns-surfacing-in-trans-pacific-partnership/ (May 21, 2012).

[155] See Attorney-General for Australia – Minister for Emergency Management, The Hon Nicola Roxon MP, *Privacy Laws Set to Reform*, Media Release, set-to-reform.aspx"http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Second%20Quarter/2-May-2012 – Privacy-laws-set-to-reform.aspx (May 2, 2012) (accessed Aug. 23, 2012); Attorney-General for Australia – Minister for Emergency Management, The Hon Nicola Roxon MP, *Privacy Reform Laws Introduced into Parliament*, Media Release http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Second%20Quarter/23-May-2012…Privacy-reform-laws-introduced-into-Parliament.aspx (accessed Aug. 26, 2012). See discussion *supra* nn.

[156] *See U.S. Cross-Border Data Flow Proposal Raises Privacy Questions*, *supra* n. 148; William J. Weber, *Privacy Across Borders: Concerns Surfacing in Trans-Pacific Partnership*, *supra* n. 148.

[157] *See* Vivek Kundra U.S. Chief Information Officer, *Federal Cloud Computing Strategy*, at pp. 13–14, http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf (Feb. 11, 2011).

[158] *See Cloud Computing: What are the Security Implications?*, Hearing before Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the House Committee on Homeland Security, http://homeland.house.gov/hearing/cloud-computing-what-are-security-implications (Oct. 6, 2011).

[159] *See* Business Roundtable, *Promoting Economic Growth Through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements, supra* n. 147 at pp. 5–9.

[160] *See* Keith Perine, *Businesses to W.H.: Stem Tide of Data Flow Rules*, Politico, http://www.politico.com/news/stories/0612/77190.html (June 7, 2012), *quoting* Daniel Castro.

White House approximately one year after the release of the Federal Cloud Computing strategy is intended to improve consumers' privacy protections by setting forth a framework upon which voluntary company implementation of binding and enforceable privacy policies may be based.[161] Pursuant to this framework, which is largely modelled after the APEC CBPR,[162] '[p]rivate sector participation will be voluntary and companies ultimately will choose whether to adopt a given code of conduct.'[163] Once chosen, company adherence to/compliance with its code of conduct would then be assured through a combination of agreed upon self-regulation and FTC and State Attorney General enforcement actions.[164] Such privacy concerns were focused upon at specially convened hearings during September 2011.[165]

Or, perhaps, such difficulties are the result of skilfully lobbied home country-based disguised digital protectionism, which is all the more incredulous considering the sacrifices that some globally-focused cloud service providers have already made to gain a competitive advantage. The evidence shows that several such companies which are among the vanguard of enterprise software providers and ICT standards developers (i.e., 'IGOR')[166] had previously assisted EU Member State and 'BRICS' national legislatures to promote locally and internationally, on putative 'public interest' grounds, government procurement rules expressing direct and indirect preferences for allegedly less expensive patent- or royalty-free 'SMART' technologies embedded in open national healthcare, energy, and ICT framework standards.[167] Attracted by the future possibility of securing lucrative government contracts, but without assurance that additional regulatory impositions would not be forthcoming, such companies had willingly agreed to reform their traditional IP (proprietary)-based business models in favour of the free and open source software community (FOSS)-driven 'software-as-a-service' (SaaS) business model, and also to accept a greater foreign government role in monitoring and potentially adjudicating the private RAND/FRAND IP licensing and pricing agreements they would enter into with other ICT technology vendors.[168] Given the current convoluted state of international cloud computing regulation, however, the bargain these industry members believed they had conclusively negotiated at the expense of their competitors may have very well become for them less certain and more costly than originally envisioned.

8 Conclusion: optimal clouds and international leadership are needed to mitigate the current economic drought and to generate internet-based global growth

It is indisputable that the perceived regulatory risks surrounding cloud computing technologies, like those surrounding other ICTs, if not otherwise susceptible to appropriate mitigation, can sufficiently dampen investment so as to undermine the financial viability and growth potential of such technologies in the marketplace. It has also been shown that governments' adoption of stable, predictable and long-term policy measures, including those that would 'provide a market-friendly environment by selecting the least costly ICT regulatory alternative available to lessen investors' operational and capital expenditure costs', will reduce regulatory uncertainty and related policy risks and help to facilitate private capital market planning and ICT investment,[169] including positive interest in cloud computing. Given these accepted findings, the cloud computing industry is justifiably confounded by and suspicious of the restrictiveness of several countries' emerging rules, including the EU's Proposed Data Protection Regulation which, if adopted in its 'preferred' form, would

Notes

[161] *See* White House Press Office, Office of the Secretary, *We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online*, Press Release, http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights (Feb. 23, 2012).

[162] *See* The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at p. 32, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (posted on February 2012).

[163] *Id.,* at pp. 2, 24, 27.

[164] *Id.*, at p. 29.

[165] *See Technology and Innovation Subcommittee Hearing - The Next IT Revolution?: Cloud Computing Opportunities and Challenges*, Hearing before the Subcommittee on Technology and Innovation of the House Committee on Science, Space and Technology, http://science.house.gov/hearing/technology-and-innovation-subcommittee-hearing-cloud-computing (Sept. 21, 2011); Chris Brantley & Gleen Tenney, *Policy in the Cloud: Congress Looks at the Federal Role in Cloud Computing*, IEEE USA Today's Engineer, http://www.todaysengineer.org/2011/Nov/cloud-computing.asp (November 2011).

[166] *See* Lawrence A. Kogan, *Commercial High Technology Innovations Face Uncertain Future Amid Emerging 'BRICs' Compulsory Licensing and IT Interoperability Frameworks*, 13 San Diego Intl. L.J. 201, 267 (2012), http://www.sandiego.edu/law/news/blogs_publications/publications/journals/international/archive.php?_focus=2705; http://www.itssd.org/Kogan%20SDILJ%20Final%20Proof%20-%201-19-12.pdf

[167] *Id.*, at pp. 228, 248–290.

[168] *Id.*, at pp. 246–247, 250, 292, 294.

[169] *See* Lawrence A. Kogan, *Commercial High Technology Innovations Face Uncertain Future Amid Emerging 'BRICS' Compulsory Licensing and IT Interoperability Frameworks*, *supra* n. 160 at 213.

significantly harm their chances of growing the cloud market both within Europe and beyond.[170]

Indeed, the adoption of the 'right' regulatory framework can be analogized to promoting desired economic 'rainmaking',[171] which is arguably what is needed on an international scale to help nations traverse the current global economic heavy weather. Not unlike scientific rainmaking which involves defined meteorological steps for seeding clouds to alleviate rain shortages that can periodically devastate important agricultural crops and draw down essential water basins,[172] 'economic rainmaking' can be critical to sustaining the success of business ventures and the vitality of the markets in which they operate.[173] In the context of cloud computing, economic rainmaking can be most effectively facilitated by cognizant, coherent, harmonized, non-restrictive and non-protectionist international rulemaking arrived at through use of a replicable methodological approach[174] that is designed and actually functions to hasten the expansion of cross-border cloud computing, and along with it, much-needed local industry and job growth. However, this demands clear leadership, not clouded vision.

Notes

[170] *See* Business Software Alliance, *BSA Global Cloud Computing Scorecard: A Blueprint for Economic Opportunity*, *supra* n. 68 at p. 3. *See also* Charles Babcock, *Is Cloud Computing A Global Market Yet?* Nyet, InformationWeek, http://www.informationweek.com/news/cloud-computing/infrastructure/232601278 (Feb. 22, 2012).

[171] Economic 'rainmaking' betrays a skill in generating sales leads and converting a portion of them into new business.

[172] *See* Prapaporn Srisathidtham & Wassana Wongrat, *Cloud Seeding Techniques in Eastern Region of Thailand*, 10th WMO [World Meteorological Organization] Scientific Conference on Weather Modification Bali, Indonesia (2011), http://www.wmo.int/pages/prog/arep/wwrp/new/documents/SEE.Srisathidtham_Thailand.pdf; Siriluk Chumchean & Walairat Bunthai, Testing Efficacy of Rainmaking Activities in the Northeast of Thailand, 10th WMO [World Meteorological Organization] Scientific Conference on Weather Modification Bali, Indonesia (2011), http://www.wmo.int/pages/prog/arep/wwrp/new/documents/OBS.Chumchean_Thailand.pdf; Warawut Khantiyanan, *50 Years Of Thailand Cloud Seeding Activity*, Bureau of the Royal Rainmaking and Agricultural Aviation, Bangkok, Thailand (2007), http://jcsepa.mri-jma.go.jp/outreach/20070131/Abstracts/S3_Khantiyanan.pdf and http://jcsepa.mri-jma.go.jp/outreach/20070131/Presentations/P3_Khantiyanan.pdf; *Rainmaking Efforts Ease Drought*, AFP , http://www.taipeitimes.com/News/world/archives/2005/04/15/2003250531(Apr. 15, 2005).

[173] *See* Business Software Alliance, *BSA Global Cloud Computing Scorecard: A Blueprint for Economic Opportunity*, *supra* n. 68 at p. 2.

[174] *See* Ford Harding, *Creating Rainmakers – The Manager's Guide to Training Professionals to Attract New Clients*, (Wiley & Sons, Inc., 2006), http://www.amazon.com/Creating-Rainmakers-Managers-Training-Professionals/dp/0471920738/ref=reader_auth_dp; Mike Schultz & John Doerr, *Rainmaking Conversations: Influence, Persuade and Sell in Any Situation* (Wiley & Sons, Inc., 2011), http://www.amazon.com/Rainmaking-Conversations-Influence-Persuade-Situation/dp/1452633266; Mike Schultz & John Doerr, *10 Rainmaker Principles – Get the Best from Your Sales People*, American Management Association, http://www.amanet.org/training/articles/10-Rainmaker-Principles-Get-the-Best-from-Your-Sales-People.aspx (Dec. 30, 2010).